

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for restricting use of a clipboard application, the method comprising:

determining whether a copy selection associated with designated content of a source file being displayed by a first source application has been made;

storing the designated content to the clipboard application; [[and]]

receiving a copy command associated with the copy selection, the copy command including a password associated with a user;

authenticating the user based upon the received password; and

determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to [[an]] the authenticated user, and wherein the secured file cannot be accessed without the file key.

2. (Currently Amended) The method recited in claim 1, further comprising receiving a paste selection to provide the designated content to [[the]] a second destination application.

3. (Previously presented) The method recited in claim 2, wherein the paste selection requests to paste the designated content to a destination file that is opened within the second destination application.

4. (Currently Amended) The method recited in claim 2, ~~wherein the copy selection is a copy command, and~~ wherein the paste selection is a paste command.

5. (Previously Presented) The method recited in claim 1, wherein the determining operates to determine that the source file is the secured file based on security information provided by the first source application.

6. (Previously Presented) The method recited in claim 5, wherein the determining includes determining that the security information pertains to the source document.

7-9. (Canceled)

10. (Previously Presented) The method recited in claim 47, wherein the preventing comprises:

storing predetermined content to the clipboard application instead of the designated content in response to determining that the source file is the secured file.

11. (Previously Presented) The method recited in claim 47, wherein the preventing comprises:

storing the designated content to the clipboard application in response to determining that the source file is not the secured file.

12. (Previously Presented) The method recited in claim 11, further comprising:

receiving a paste selection to provide the designated content to the second destination application.

13-15. (Canceled)

16. (Currently Amended) A method for restricting use of a clipboard application, the method comprising:

receiving a copy selection associated with designated content of a source file being displayed by a first source application;

receiving a copy command associated with the copy selection, the copy command including a password associated with a user;

authenticating the user based upon the received password; and

determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to [[an]] the authenticated user, and wherein the secured file cannot be accessed without the file key, wherein said determining is performed by one or more computing devices.

17. (Previously presented) The method recited in claim 16, further comprising storing alternate content to the clipboard application in response to determining that the source file is the secured file.

18. (Previously Presented) The method recited in claim 17, wherein the alternate content is one or more of blank content, predetermined content, or scrambled content.

19. (Previously Presented) The method recited in claim 17, further comprising:

supplying the predetermined content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is not the secured file.

20. (Previously presented) The method recited in claim 16, wherein further comprising:

supplying the designated content to the clipboard application in response to-determining that the source file is not the secured file.

21. (Previously Presented) The method recited in claim 20, wherein the determining operates to determine that the source file is the secured file based on security information provided by the first source application.

22. (Previously Presented) The method as recited in claim 21, wherein the determining includes determining that the security information pertains to the source document.

23 - 39. (Canceled)

40. (Currently Amended) A non-transitory tangible computer readable medium having instructions stored thereon for restricting the use of a clipboard application, the instructions comprising:

instructions to receive a copy selection associated with designated content of a source file being displayed by a first source application;

instructions to receive a copy command associated with the copy selection, the copy command including a password associated with a user;

instructions to authenticate the user based upon the received password;
and

instructions to determine whether the source file is a secured file, wherein the secured file includes a header having a file key available to [[an]] the authenticated user, and wherein the secured file cannot be accessed without the file key.

41. (Currently Amended) The non-transitory computer readable medium ~~method~~ recited in claim 51, wherein said instructions to prevent comprise:

instructions to store blank content to the clipboard application in response to determining that the source file is a secured file.

42. (Currently Amended) The non-transitory computer readable medium ~~method~~ recited in claim 51, wherein said instructions to prevent comprise:

instructions to store the designated content to the clipboard application in response to determining that the source file is not a secured file.

43. (Currently Amended) The non-transitory computer readable medium ~~method~~ recited in claim 41, wherein said method further comprises:

receiving a paste selection to provide the designated content to the second destination application;

supplying the blank content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is a secured file; and

supplying the designated content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is not a secured file.

44. (Previously Presented) The method recited in claim 47, wherein said preventing comprises:

storing scrambled content to the clipboard application in response to determining that the source file is a secured file.

45. (Previously Presented) The method recited in claim 47, wherein said preventing comprises:

storing the designated content to the clipboard application in response to determining that the source file is not a secured file.

46. (Previously presented) The method recited in claim 45, further comprising:

receiving a paste selection to provide the designated content to the second destination application;

supplying the scrambled content from the clipboard application to the second destination application in response to the paste selection if said determining determines that the source file is a secured file; and

supplying the designated content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is not a secured file.

47. (Previously Presented) The method recited in claim 1, further comprising:
preventing subsequent usage of the designated content in a second destination application via the clipboard application in response to determining that the source file is a secured file.

48. (Previously Presented) The method recited in claim 12, further comprising:

supplying the predetermined content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is a secured file.

49. (Previously Presented) The method recited in claim 12, further comprising:

supplying the designated content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is not a secured file.

50. (Previously Presented) The method recited in claim 16, further comprising:

preventing subsequent storage of the designated content to a second destination application via the clipboard application in response to determining that the source file is the secured file.

51. (Currently Amended) The non-transitory ~~tangible~~ computer readable medium of claim 40, the instructions further comprising:

instructions to prevent subsequent usage of the designated content in a second destination application via the clipboard application in response to determining that the source file is a secured file.